UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/833,005	04/12/2001	Douglas A. Hardy	GE04591	9509

7590 02/01/2007

Stanley A. Schlitter
JENNER & BLOCK, LLC
One IBM Plaza
Chicago, IL 60611

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	PAPER NUMBER
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 09/833,005	**Applicant(s)** HARDY ET AL.	
	Examiner Eleni A. Shiferaw	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 November 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☒ Claim(s) *21-30* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)	4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) □ Notice of Informal Patent Application
3) □ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.	6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/24/2006 has been entered.

2. Claims 1-30 are pending.

Response to Amendment/Arguments

3. Applicant's amendments and arguments with respect to amended claims 1, and 11, and newly added claims 21-30 filed 11/24/2006 have been fully considered but are moot in view of the new ground(s) of rejection.

Applicant's arguments with respect to claim 1, and 11 have been considered but they are not persuasive. Regarding applicant's argument wherein reference Chou failure to disclose that the decryption key K being the same key used to initially encrypt the software product, argument is not persuasive, because Chou discloses a method of distributing encrypted software using encrypting key (see, col. 2 lines 47-col. 3 lines 50). The key used to encrypt, key k, is a combination of k1 and k2 (see, col. 4 lines 10-54). k1 is generated in the user's device and transmitted to central processing unit (see, col. 4 lines 12-19) and k2 is generated in a processing center device from decrypting key and k1 (see, col. 4 lines 19-22), in order to provide a decryption key k by combining k1 and k2 (see, col. 4 lines 24-54). The user generates integral unique key based on K2 receivęd and compares with same factor from installation file and determines unique factors (col. 4 lines 27-40). The user device combines K1 and K2 to form decryption key K and uses to decrypt the software (col. 4 lines 41-49). Since k2 is generated from key k/decryption key and k1 (col. 4 lines 20-22) and decryption is not performed if the combination of the received k2 and k1 does not produce key k/decryption key (col. 4 lines 50-54), decryption key is the same as encryption key. If k2 is generated from key k/encryption key/decryption key and k1 ➔ key k/encryption key/decryption key can be generated from k1 and k2 and therefore key k/encryption key/decryption key in both equation are the same.

Regarding argument wherein first key portion is generated independent user's hardware product, new ground of rejection is provided, as recited in claims 1, and 11.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-2 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al. (Chou, EP 0 636 962 A2) in view of Torrubia-Saez US 6,966,002 B1.

As per claim 1, Chou teaches method for enabling encryption and decryption of an initial version of a software product comprising the steps of:

generating a first encryption key (col. 3 lines 44-50; *encryption key*);

encrypting the initial version of the software product with said first encryption key to generate an encrypted initial software product (col. 2 lines 48-51; *different encryption key encrypting a software*);

splitting said first encryption key into first and second key portions (fig. 1 element 14 and 16; *K1 and K2*) by (i) generating a first key portion of said first encryption key (col. 4 lines 11-14; *generating first key portion: K1*); and (ii) calculating a second key portion by utilizing said first key portion and said first encryption key to generate said second key portion of said first encryption key such that the combination of said first key portion and second key portion form said first encryption key (col. 4 lines 19-24; *generating the second key portion K2 from K1 and decryption key K, decryption key K/encryption key could not decrypt the software without first calculation the second potion and combining the calculated second portion with the received first portion*);

providing said first key portion and said second key portion and said encrypted initial software product for use in a hardware product (col. 3 lines 49-col. 4 lines 49; *encrypted software, K1 and K2 are provided to a user from processing center*);

combining said first key portion and said second key portion to provide said first encryption key in said hardware product (col. 4 lines 45-49, and col. 5 lines 8-9; *combing K1 and K2*); and utilizing said first encryption key to decrypt said encrypted initial software product in said hardware product (col. 5 lines 51-54, and col. 6 lines 25-28; *using decryption key/encryption key to decrypt encrypted software*).

Chou fails to disclose the key portion is independent of the hardware product.

However Torrubia-Saez discloses decryption key is splitted into two parts, of which one part is calculated in the server, and the other part is calculated in the users computer (see col. 18 lines 40-57).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Torrubia-Saez within the system of Chou because they are analogous in split key generation and software encryption. One would have been motivated to incorporate the teachings of Torrubia-Saez within the system of Chou because it is well known to generate a portion of the splitted key in a first device and to generate the second key portion in a second device to produce a decryption key.

Regarding claim 2, Chou discloses the method wherein said step of generating a first encryption key utilizes a ransom number generator to generate said first encryption key (col. 3 lines 49-col. 4 lines 14).

6. Claims 3-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al. (Chou, EP 0 636 962 A2) in view of Torrubia-Saez US 6,966,002 B1 and further in view of Rasmussen et al. Patent Number: 5,301,247.

Regarding claim 3 Chou teaches the method wherein said step of calculating a second key portion and combining the first key portion and the first encryption key/decryption key to calculate the second key portion (col. 4 lines 10-26). Chou does not disclose an "exclusive or" operator to combine the keys to calculate second key portion.

However using an "exclusive or" operator to combine key portions is very well known and Rasmussen teaches it (see, fig. 4 element 144 and col. 8 lines 40-48; *xoring first portion of key (DEK1) with second portion (DEK2) of key to form encryption key (DEK)*).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of excusive or within the combination system to combine the first encryption key and first key portion because operator exclusive or necessary for combining. One would have been motivated to do so to combine the first splitted portion of the key with the encryption key/decryption key.

Regarding claim 4 Rasmussen further discloses wherein said step of combining said first key portion and said second key portion utilizes an "exclusive or" logic operation to combine said first key portion and said second key portion to provide said first encryption key (see, fig. 4 element 144 and col. 8 lines 40-48; *xoring first portion of key (DEK1) with second portion (DEK2) of key to form encryption key (DEK)*). The rational for combining are the same as claim 3 above.

7. Claims 5-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al. (Chou, EP 0 636 962 A2), and Torrubia-Saez and further in view of Kitajima et al. (Kitajima, Patent No.: US 6,823,069 B1).

As per claim 5, Chou and Torrubia-Saez teach the method further enabling of said first encryption key to provide a second encryption key to secure a different version of the initial software product, further comprising the steps of:

generating the second encryption key (Chou col. 3 lines 44-50; *encryption key*);

encrypting the different version of the initial software product with the second encryption key to provide an encrypted different version of the software product (Chou col. 2 lines 48-51; *different encryption key encrypting a software*);

combining the first encryption key and the second encryption key to provide a third key portion (Chou col. 4 lines 19-24; *combining K1 and decryption key/encryption key*);

installing said third key portion and the encrypted different version of the software product in said hardware product (Chou col. 2 lines 2-9 and col. 4 lines 11-26; *generating first key and sending/storing the generated first key to the external central processing system*);

combining said third key portion and said second key portion to generate a fourth key portion in said hardware product (Chou col. 4 lines 45-49, and col. 5 lines 8-9; *combing K1 and K2*);

combining the first key portion and the fourth key portion to provide said second encryption key in said hardware product (Chou col. 4 lines 19-24); and

using the second encryption key to decrypt the encrypted different version of the software product (Chou col. 4 lines 45-49, and col. 5 lines 8-9; *combing K1 and K2*).

Chou and Torrubia-Saez fail to teach an update of the keys.

However Kitajima discloses dividing encrypting key into a first half portion and a second half portion and periodically updating/changing keys and encryption algorithm to securely protect cryptograms against unauthorized people (col. 11 lines 1-10).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of updating keys within the combination system because it would allow a secure data/message/information transmission (col. 11 lines 1-10). One would have been motivated to update the encryption key and the key portions to enhance security by making the keys unpredictable.

As per claim 6, Chou discloses the method wherein said step of generating a first encryption key utilizes a ransom number generator to generate said first encryption key (col. 3 lines 49-col. 4 lines 14).

8. Claims 7-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al. (Chou, EP 0 636 962 A2), Torrubia-Saez US 6,966,002 B1 and Kitajima et al. (Kitajima, Patent No.: US 6,823,069 B1), and further in view of Rasmussen et al. Patent Number: 5,301,247).

As per claim 7, Chou and Kitajima teach all the subject matter as described above. Chou and Kitajima fail to disclose exclusive or operator.

However Rasmussen using an "exclusive or" operator to combine key portions is very well known and Rasmussen teaches it (see, fig. 4 element 144 and col. 8 lines 40-48; *xoring first portion of key (DEK1) with second portion (DEK2) of key to form encryption key (DEK)*).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of excusive or within the combination system of Chou and Kitajima to combine said first encryption key and said second encryption key and generate said third key portion because operator exclusive or necessary for combining. One would have been motivated to do so to combine first encryption key and said second encryption key.

As per claim 8, the combination teaches wherein said step of providing said second encryption key utilizes an "exclusive or" logic operation to combine said first key portion and said fourth key portion to provide said second encryption key (see, Rasmussen fig. 4 element 144 and col. 8 lines 40-48; *xoring first portion of key (DEK1) with second portion (DEK2) of key to form encryption key (DEK) and Chou col. 4 lines 10-26*). The rational for combining are the same as claim 7 above.

9. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al. (Chou, EP 0 636 962 A2), Torrubia-Saez US 6,966,002 B1and Kitajima et al. (Kitajima, Patent No.: US 6,823,069 B1) and further in view of Vincent Pub. No.: US 2004/0015953 A1.

As per claim 9, Chou, Torrubia-Saez, and Kitajima disclose all the subject matter as described above. Chou, Torrubia-Saez and Kitajima fail to disclose wherein said initial version of software product and said different version of said initial version of said software product are non-sequential versions.

However Vincent discloses updating required versions out of multiple different versions of software products in non-sequential order (fig. 9 and par. 0071; *updating component B from version 4 to version 6 and updating full component of D and E to version 1 and 2 respectively*).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Vincent within the combination system because it would save time (par. 0015). One would have been motivated to update non-sequential version of software because it would allow a minimal time to download specific software components in contrast to conventional methods of updating software (par. 0015).

10. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al. (Chou, EP 0 636 962 A2) in view of Torrubia-Saez US 6,966,002 B1 and Kitajima et al. (Kitajima, Patent No.: US 6,823,069 B1), and further in view of Mizikovsky Patent No.: US 6,853,729 B1.

Regarding claim 10, Chou, Torrubia-Saez and Kitajima disclose all the subject matter as described. Chou, Torrubia-Saez and Kitajima fail to teach wherein the second encryption key is non-sequential with said first encryption key. However Mizikovsky teaches an update key which is non-sequential with said first encryption key (col. 8 lines 21-43 and fig. 4; *update key being different from new key...generated in using RAND numbers*).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of Mizikovsky within the combination system because it would enhance security. One would have been motivated to incorporate the teachings of updating keys in non-sequential order to prevent unauthorized device from learning encryption keys and perform unauthorized decryption of content.

11. Claims 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al. (Chou, EP 0 636 962 A2) in view of Chan Patent Number: 5,150,407 and Torrubia-Saez US 6,966,002 B1.

As per claim 11 a method for providing for the security of encryption keys for encryption and decryption of an initial version of a software product provided by a provider to a user of a hardware product, said method comprising:

providing a first encryption key (col. 3 lines 44-50; *encryption key*);

encrypting the initial version of the software product with said first encryption key to generate an encrypted initial software product (col. 2 lines 48-51; *different encryption key encrypting a software*);

splitting said first encryption key into first and second key portions (fig. 1 element 14 and 16; *K1 and K2*) by (i) providing a first key portion (col. 4 lines 11-14; *generating first key portion: K1*); and (ii) utilizing said first key portion and said first encryption key to calculate a second key portion of said first encryption key such that the combination of said first and second key portions form said first encryption key (col. 4 lines 19-24; *generating the second key portion K2 from K1 and decryption key K, decryption key K/encryption key could not decrypt the software without first calculation the second potion and combining the calculated second portion with the received first portion*);

storing said first key portion in storage means external to the hardware (col. 2 lines 2-9 and col. 4 lines 11-26; *generating first key and sending/storing the generated first key to the external central processing system*);

storing said encrypted software product in a further memory means in the hardware product (col. 1 lines 40-col. 2 lines 9; *stored software distribution*);

combining said first key portion and said second key portion in the hardware product to provide said first encryption key (col. 4 lines 45-49, and col. 5 lines 8-9; *combing K1 and K2*); and

decrypting said encrypted initial software product with said first encryption key (col. 5 lines 51-54, and col. 6 lines 25-28; *using decryption key/encryption key to decrypt encrypted software*).

Chou teaches *encrypted software with encryption key, encryption key is divided in to two portions, K1 and K2, k1 is generated in user's device, and the other portion of the key, K2, calculated on the processing center is transmitted to user's device to decrypt the encrypted software by combining K1 and K2* (col. 2 lines 48-57 and col. 4 lines 10-31). However Chou does not explicitly disclose storing said second key portion separately from said first key portion in a tamper proof memory means in the hardware product;

However Chan teaches encrypting digital data using encryption key, dividing encryption key in to two portions (col. 5 lines 44-45) and storing the portions of the key in two different storage devices (col. 5 lines 45-47, and col. 9 lines 6-14), and combining the portions of the keys in order to decrypt the encrypted digital data (col. 9 lines 28-30).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Chan within the system of Chou because it would enhance security (col. 5 lines 17-63). One would have been motivated to do so for secure use of decryption keys and data protection and/or the user cannot access the other portion easily.

Chou and Chan fail to explicitly disclose the key portion is independent of the hardware product.

However Torrubia-Saez discloses decryption key is splitted into two parts, of which one part is calculated in the server, and the other part is calculated in the users computer (see col. 18 lines 40-57).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Torrubia-Saez within the combination system because they are analogous in split key generation and software encryption. One would have been motivated to incorporate the teachings of Torrubia-Saez within the combination system because it is well known to generate a portion of the splitted key in a first device and to generate the second key portion in a second device to produce a decryption key.

Regarding claim 12, Chou further discloses the method wherein said step of generating a first encryption key utilizes a ransom number generator to generate said first encryption key (col. 3 lines 49-col. 4 lines 14).

12. Claims 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al. (Chou, EP 0 636 962 A2), Chan Patent Number: 5,150,407, and Torrubia-Saez US 6,966,002 B1 and further in view of Rasmussen et al. Patent Number: 5,301,247).

As per claim 13, Chou, Chan and Torrubia-Saez teach the method wherein said step of calculating a second key portion and combining the first key portion and the first encryption key/decryption key to calculate the second key portion (Chou col. 4 lines 10-26). Chou, Chan and Torrubia-Saez do not disclose an "exclusive or" operator to combine the keys to calculate second key portion.

However using an "exclusive or" operator to combine key portions is very well known and Rasmussen teaches it (see, fig. 4 element 144 and col. 8 lines 40-48; *xoring first portion of key (DEK1) with second portion (DEK2) of key to form encryption key (DEK)*).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of excusive or within the combination system to combine the first encryption key and first key portion because operator exclusive or necessary for combining. One would have been motivated to do so to combine the first splitted portion of the key with the encryption key/decryption key.

As per claim 14, the combination teaches wherein said step of combining said first key portion and said second key portion utilizes an "exclusive or" logic operation performed by said hardware product (Rasmussen fig. 4 element 144 and col. 8 lines 40-48; *xoring first portion of* *key (DEK1) with second portion (DEK2) of key to form encryption key (DEK) and Chou col. 4 lines 10-26*) The rational for combining are the same as claim 13 above.

13. Claims 15-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al. (Chou, EP 0 636 962 A2), Chan Patent Number: 5,150,407, and Torrubia-Saez teach and further in view of Kitajima et al. (Kitajima, Patent No.: US 6,823,069 B1).

As per claim 15, Chou, Chan and Torrubia-Saez teach all the subject matter as described above. In addition the combination discloses the method further enabling security of said first encryption key and providing a second encryption key for encrypting a different version of the initial software product, further comprising:

generating the second encryption key (Chou col. 3 lines 44-50; *encryption key*);

encrypting the different version of the initial software product with said second encryption key to provide an encrypted different version of the initial software product (Chou col. 2 lines 48-51; *different encryption key encrypting a software*);

combining said first encryption key and said second encryption key to provide a third key portion (Chou col. 4 lines 19-24; *combining K1 and decryption key/encryption key*);

installing said third key portion in said tamper proof memory means (Chan col. 5 lines 45-47, and col. 9 lines 6-14);

installing said encrypted different version of the initial software product in said further memory means in the hardware product (Chou col. 1 lines 40-col. 2 lines 9; *stored software distribution*);

combining said third key portion and said second key portion to generate a fourth key portion in the hardware product (Chou col. 4 lines 45-49, and col. 5 lines 8-9; *combing K1 and K2*);

combining said first key portion and said fourth key portion to provide said second encryption key in the hardware product (Chou col. 4 lines 19-24); and

using said second encryption key in the hardware product to decrypt the encrypted different version of the initial software product (Chou col. 4 lines 45-49, and col. 5 lines 8-9; *combing K1 and K2*). The rational for combining are the same as claim 11 above.

Chou, Chan, Torrubia-Saez fail to teach an update of the keys.

However Kitajima discloses dividing encrypting key into a first half portion and a second half portion and periodically updating/changing keys and encryption algorithm to securely protect cryptograms against unauthorized people (col. 11 lines 1-10).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of updating keys within the combination system because it would allow a secure data/message/information transmission (col. 11 lines 1-10). One would have been motivated to update the encryption key and the key portions to enhance security by making the keys unpredictable.

As per claim 16, Chou further discloses the method wherein said step of generating a first encryption key utilizes a ransom number generator to generate said first encryption key (col. 3 lines 49-col. 4 lines 14).

14. Claims 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al. (Chou, EP 0 636 962 A2), Chan Patent Number: 5,150,407, Torrubia-Saez and Kitajima et al. (Kitajima, Patent No.: US 6,823,069 B1) and further in view of Rasmussen et al. Patent Number: 5,301,247.

As per claim 17, Chou, Chan, Torrubia-Saez and Kitajima disclose all the subject matter as described above. Chou, Chan, Torrubia-Saez and Kitajima fail to disclose exclusive or operator.

However Rasmussen using an "exclusive or" operator to combine key portions is very well known and Rasmussen teaches it (see, fig. 4 element 144 and col. 8 lines 40-48; *xoring first portion of key (DEK1) with second portion (DEK2) of key to form encryption key (DEK)*).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of excusive or within the combination system to combine said first encryption key and said second encryption key and generate said third key portion because operator exclusive or necessary for combining. One would have been motivated to do so to combine first encryption key and said second encryption key.

As per claim 18, the combination teaches wherein said step of combining said first key portion and the fourth key portion to provide said second encryption key utilizes an "exclusive or" logic operation (see, Rasmussen fig. 4 element 144 and col. 8 lines 40-48; *xoring first portion of key (DEK1) with second portion (DEK2) of key to form encryption key (DEK) and Chou col. 4 lines 10-26*). The rational for combining are the same as claim 17 above.

15. Claims 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al. (Chou, EP 0 636 962 A2) and Chan Patent Number: 5,150,407, Torrubia-Saez and Kitajima et al. (Kitajima, Patent No.: US 6,823,069 B1) and further in view of Vincent Pub. No.: US 2004/0015953 A1.

Regarding claim 19, Chou, Chan, Torrubia-Saez and Kitajima disclose all the subject matter as described. Chou, Chan, Torrubia-Saez and Kitajima fail to disclose wherein said initial version of software product and said different version of said initial version of said software product are non-sequential versions.

However Vincent discloses updating required versions out of multiple different versions of software products in non-sequential order (fig. 9 and par. 0071; *updating component B from version 4 to version 6 and updating full component of D and E to version 1 and 2 respectively*).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Vincent within the combination system because it would save time (par. 0015). One would have been motivated to update non-sequential version of software because it would allow a minimal time to download specific software components in contrast to conventional methods of updating software (par. 0015).

16. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chou et al. (Chou, EP 0 636 962 A2), Chan Patent Number: 5,150,407, Torrubia-Saez and Kitajima et al. (Kitajima, Patent No.: US 6,823,069 B1) and further in view of Mizikovsky Patent No.: US 6,853,729 B1.

Regarding claim 20, Chou, Chan, Torrubia-Saez and Kitajima disclose all the subject matter as described. Chou, Chan, Torrubia-Saez and Kitajima fail to teach wherein the second encryption key is non-sequential with said first encryption key. However Mizikovsky teaches an update key which is non-sequential with said first encryption key (col. 8 lines 21-43 and fig. 4; *update key being different from new key...generated in using RAND numbers*).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of Mizikovsky within the combination system because it would enhance security. One would have been motivated to incorporate the teachings of updating keys in non-sequential order to prevent unauthorized device from learning encryption keys and perform unauthorized decryption of content.

Allowable Subject Matter

17. Claims 21-25 and 26-30 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure Pub. No.: US 2001/0001876 A1: *Morgan et al. discloses a well-known splitting key method i.e. splitting key in to parts.*

Please see PTO 892 form for further prior art of record.

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

January 29, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/29/07